February 12, 2018

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

RE: EB Docket No. 06-36
Annual CPNI Certification

Dear Ms. Dortch:

Attached is the annual CPNI certification filing covering the year of 2017, pursuant to 47 C.F.R § 64.2009(e), for West River Telecommunications Cooperative, 803331.

Sincerely,

Michelle Perreault

Michelle Perreault
Personnel Director

Attachment

Annual 47 CFR § 64.2009(e) CPNI Certification Template

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

1. Date filed: February 12, 2018
2. Name of company(s) covered by this certification: West River Telecommunications Cooperative
3. Form 499 Filer ID: 803331
4. Name of signatory: Troy Schilling
5. Title of signatory: CEO
6. Certification:

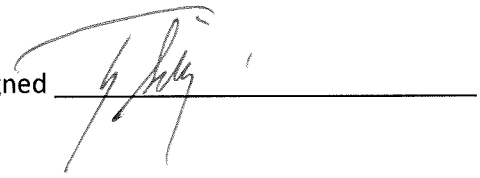
I, Troy Schilling, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 CFR § 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 et seq. of the Commission's rules.

The company has not taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 

Attachments: WRT Policy 512

WEST RIVER TELECOMMUNICATIONS COOPERATIVE

CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)

I. OBJECTIVE

To establish and explain operating procedure for compliance with Customer Proprietary Network Information (CPNI) rules.

A. DEFINITIONS

CPNI is – Information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier. It is information made available to the carrier by the customer solely by virtue of the carrier-customer relationship. Examples are: sensitive personal information; types of services purchased; optional services used; phone numbers called; time, date and duration of calls; calling patterns; frequently called states; amount the customer spends on communication services; and type of network to which the customer subscribes.

CPNI is not - Subscriber list information, aggregate information or information we get from customers in ways other than through the provision of service. Examples are: customer information listed in the telephone directory; collective data that relates to a group or category of services or customers from which individual identifying characteristics have been removed; and public records obtained from a courthouse.

Call Detail Information is - Information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

Call Detail Information is not – Products, types of service customer subscribes to, technical configuration or amount customer owes.

II. CONTENT

WRT (the "Company") has implemented the following procedures to ensure that it is compliant with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), § 64.2001 through § 64.2011.

A. Compliance Officer

The Company has appointed a CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Company is in compliance with all of the CPNI rules. The Compliance Officer is also the point of contact for anyone (internally or externally) with questions about CPNI.

B. **Employee Training**

The Compliance Officer arranges for the training of all employees on an annual basis, and more frequently as needed. Any new employee is trained when hired by the Company. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the company is using. The detail of the training can differ based on whether or not the employee has access to CPNI.

After the training, all employees are required to sign a certification that they have received training on the CPNI rules, that they understand the Company's procedures for protecting CPNI and they understand the Company's disciplinary process for improper use of CPNI.

Employees are instructed that if they ever have any questions regarding the use of CPNI, or if they are aware of CPNI being used improperly by anyone, they should contact the Compliance Officer immediately.

C. **Disciplinary Process**

The Company has established a specific disciplinary process for improper use of CPNI. The disciplinary action is based on the type and severity of the violation and could include any or a combination of the following: retraining the employee on CPNI rules, notation in the employee's personnel file, formal written reprimand, suspension or termination.

Any employee that knowingly causes a "breach" (when a person without authorization, or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI or intentionally uses CPNI to do harm to a customer or to obtain self-profit from use of the CPNI) will be subject to immediate termination.

The disciplinary process is reviewed with all employees.

D. **Customer Notification and Request for Approval to Use CPNI**

The Company has provided notification to its customers of their CPNI rights and has asked for the customer's approval to use CPNI via the opt-out method. A copy of the notification is also provided to all new customers that sign up for service.

The status of a customer's CPNI approval is prominently displayed as soon as the customer's account is accessed so that employees can readily identify customers that have restricted the use of their CPNI.

For the customers that have opted-out and said the Company cannot use their CPNI, that decision will remain valid until the customer changes it.

The Company sends the opt-out notice every two years to those customers that have not previously opted out.

The Company will provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

A copy of the most recent notification is kept in the CPNI official files.

E. Marketing Campaigns

If the Company uses CPNI for any marketing campaign, the Compliance Officer will review the campaign and all materials to ensure that it is in compliance with the CPNI rules.

The Company has a process for maintaining a record of any marketing campaign of its own, or its affiliates, which uses customers' CPNI.

F. Authentication

The Company does not disclose any CPNI until the customer has been appropriately authenticated as follows:

1. **In-office visit** - the customer must provide a valid photo ID matching the customer's account information.

2. **Customer-initiated call if using a password** – the customer must provide his/her pre-established password and must be listed as a contact on the account. If the customer cannot provide the password or the answer to the back-up authentication, the customer is re-authenticated, without using readily available biographical information or account information, and a new password is established.

3. **Customer-initiated call if not using a password** – the customer is authenticated by providing an answer to a pre-established question and must be listed as a contact on the account.

   If the customer wants to discuss call detail information that requires a password, the following guidelines are followed:

- If the customer can provide all of the call detail information (telephone number called, when it was called, and the amount of the call) necessary to address the customer's issue, the Company will continue with its routine customer care procedures.

- If the customer cannot provide all of the call detail information to address the customer's issue, the Company will: (1) call the customer back at the telephone number of record, (2) send the information to the address of record, or (3) ask the customer to come into the office and provide a valid photo ID.

4. **Written request for Call Detail Information –** The customer may request that call detail information (incoming or outgoing call records) be released to the address of record.

G. Notification of Account Changes

The Company promptly notifies customers whenever a change is made to any of the following:

- Password
- Customer response to a back-up means of authentication for a password.
- Online account.
- Address of record.

The notification to the customer will be made either by a Company-originated voicemail or text message to the telephone number of record or sent to the address (postal or electronic) of record.

The Company has a process for tracking when a notification is required and for recording when and how the notification is made. When a change is made to a customer's record a Customer Service Representative will notify the customer in writing that a change has been made to their account. The letter is sent to the address of record and a copy of the letter is placed into the Company's read file.

H. Notification of Breaches

Employees will immediately notify the Compliance Officer of any indication of a breach. If it is determined that a breach has occurred, the Compliance Officer will do the following:

- Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but in no event later than 7 business days after determination of the breach. The notification will be via the FCC link at http://www.fcc.gov/eb/cpni.

- Notify customers only after 7 full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested an extension.

- If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency.

- Maintain a record of the breach, the notifications made to the USSS and FBI, and the notifications made to customers. The record should include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

- Include a summary of the breach in the annual compliance certificate filed with the FCC.

I. Annual Certification

The Compliance Officer will file a Compliance Certification with the FCC by March 1 of each year, for data pertaining to the previous calendar year.

J. Record Retention

The Company retains all information regarding CPNI in a CPNI file. Following is the minimum retention period established for specific items:

- CPNI notification and records of approval – one year
- Marketing campaigns – one year
- Breaches – two years
- Annual certification – five years
- Employee training certification – two years
- All other information – two years